## REMARKS

Applicants appreciate the telephone conference with Examiner Tsai, and in accordance with our letter of October 28, 2003 explaining the declaration signatures, it is believed that this issue is now moot. If there are any remaining issues on the declaration, the undersigned attorney would appreciate a telephone conference.

The present invention is directed to an improvement in securing a multi-layer board carrying components to increase its tamper resistance to unauthorized parties. The present invention specifically attempts to address a relatively economical solution to this problem without significantly increasing the cost, by providing the ability to use conventional existing components, without requiring the logics for encryption and decryption to be embedded into corresponding components, and without embedding the resulting multi-layer board in significant amounts of resin.

Within these parameters, the present invention achieves a highly tamper-resistance multi-layer board wherein signal lines requiring tamper resistance are rendered difficult to be accessed by contact probing by an unauthorized user.

The species that were elected in the restriction requirement can be seen, for example, in Figures 1 through 3 of our present drawings. The claims have now been further amended consistence with this disclosure and to distinguish over the cited art.

The Office Action rejected Claims 1-6 as being completely anticipated by the *Benson et al.* (U.S. Publication 2002/0002683).

The *Benson et al.* reference taught the insertion of both passive security features and active security features that would function together to provide a heightened degree of security against tampering. In the embodiments cited in the Office Action, the specific security module

comprised a substrate and a cover within an embedded three-dimensional resistive network sensor comprising a multiplicity of serial conductive paths which are integral to both the substrate and the cover. More particularly, multiple layers of inter-digitated serpentine serial conductor paths were made integral to the laminates of the substrate and the cover. These multiply serial conductive paths essentially surround the electronic components within the enclosure formed by the substrate and the cover 106. As an additional advantage, a parasitic capacitance can be deployed between the outermost layer of serpentine serial conductor paths in the substrate and cover 106 and its associated laminated metallic cover. Modification of this capacitance can act as an additional sensor to monitor the tamper detection circuits including key zeroing electronics that can destroy or erase any sensitive programs or data.

The Office Action specifically referred to a signal line including the conductive trace 134 shown in Figure 3D and the conductive via 136 shown in Figure 3C. As disclosed in column 5, the serpentine serial conductive paths which are generically referred to by numeral 134 basically run substantially across the entire metallization layer in a pseudo-random manner. See page 5, paragraph 70. The vias shown in Figure 3C form part of a picket fence configuration.

The Office Action also cited the teaching in Figure 6B, electronic component 162, which is taught as an alternative embodiment in the *Benson et al.* disclosure. In this embodiment, element 158 is the top cover, and element 160 is the bottom cover that sandwiches a substrate 156.

As noted, the electronic components 162 are generically described as being attached to both sides of the substrate 156. The top cover and the bottom cover are formed of an opaque material to effectively obscure any patterns of conductors formed in the substrate. Additionally, each of these covers include the multiple layers of inter-digital serpentine serial conductor paths,

as seen in Figure 3D, as elements 134. Accordingly, simply stating, as set forth in the rejection, that an electronic component is mounted on an outside layer does not address the features of the present invention as set forth in our present claims.

While a configuration of serpentine serial conductor paths is taught in the *Benson et al.* reference may produce in essence a "Faraday cage" around the protected electronic components, it would not address the economical solution of a resulting multi-layer board as defined in our currently elected species.

Referring, for example, to Claims 1 and 6, portions of the signal line existing on the outside layer of our multi-layer board are covered only by a predetermined component to which the signal line is connected, but not otherwise on the other areas of the outside layer. This arrangement provides a particularly advantageous characteristic of preventing an increase in production cost and of enhancing against any unauthorized contact probing at the outside layer of the multi-layer board. Our present invention prevents an increase in production costs because portions of the signal line existing on the surface of the board are covered only by such components that are originally required for the circuit operation, and thus there is no need to deposit any new members to cover the portions of the signal line. For example, if a resin, not necessary for the circuit operation, is used to cover the signal line appearing on the board surface, it would naturally increase both time and production costs.

The cited teachings in the *Benson et al.* reference can be characterized as providing a security module that would include a signal line requiring tamper resistance (conductive path 134 as shown in Figure 3D). A conductive via passes through layers of the multi-layer board (via 136 as shown in Figure 3C), circuit components (electrical components 162 shown in Figure

6H) and a cover 106 (shown in Figure 2). All signal line and components are further covered by the cover 106 that is not necessary for the circuit operation.

Thus, the *Benson et al.* reference, while showing and teaching multiple active and passive tamper-resistant components neither discloses nor suggests the construction of the present invention in which portions of the signal line appearing in the layer are covered only by such components that are originally required for the circuit operation, for example, electric components 162 shown in Figure 6B.

To complete the multi-layer board of the *Benson et al.* reference and to secure the tamper-resistance features, it is required to mount electronic components on the substrate 104 and then further to attach the cover 106 to the composite member as shown in Figure 2. The time, effort and additional material cost for this multi-layer board with serpentine serial conductor paths would be far larger than that for multi-layer board defined by our presently pending claims.

The Office Action further rejected Claim 30 as being completely anticipated by the *McCalley et al.* (U.S. Patent No. 5,956,415). This reference was cited purportedly for its teaching of a tamper-resistance multi-layer board for the transfer of pixel data to be encrypted, and in this regard, it teaches a fingerprint sensor package with a tamper-resistance housing. The fingerprint sensor is mounted within the housing along with the encryption output circuit.

For the purpose of enhancing security, predetermined patterns of fingerprints that define authorized users can be stored in a module wherein any unauthorized contact can destroy this information to safeguard the system. See, for example, the teaching on column 12, lines 51-64. Thus, breaching the housing permits the memory 198 or other integrated circuit components to be destroyed or rendered secure. Specifically, a coating 193 of a material may be applied to the

integrated circuit die that causes destruction of the die if the coating is dissolved away. The memory 193 can also self-destruct or empty its contents upon exposure to light or upon removal of any sustaining electric circuit.

Although the Office Action cites a conductive path as purportedly positioned underneath a processor and destructive memory as shown in Figure 122 to prevent direct access from the exterior of the board, it is clear that there is no support, for example, in column 12 of the *McCalley et al.* patent for such a position, let alone a teaching to render our current claims as anticipated.

Referring specifically to Claim 30, portions of the conductive path interconnecting the reception/decryption unit and the output interface unit (that is, a signal line requiring tamper resistance) that are not positioned adjacent an interior layer surface are positioned under the reception/decryption unit and/or the output interface unit only. This feature of the present invention prevents an increase in production cost and has the capability of enhancing resistance to contact probing at an outside layer of the multi-layer board.

In contrast, the *McCalley et al.* reference relied upon a tamper-resistant housing 191 that is not necessary for the circuit operation as shown in Figure 22. Components such as the substrate 195, processor 192 mounted on the substrate, a destructible memory 193, and the encrypted output circuit 194 are covered with a tamper-resistant housing 191. There is no teaching nor suggestion in the *McCalley et al.* reference that portions of a signal line interconnecting the processor 192 and the encrypted output circuit 194 are positioned adjacent an interior layer surface and are covered with a processor 192 in the encrypted output circuit 194.

To complete the sensor package 190 of the *McCalley et al.* reference, it is required to mount components in the substrate 195 and then to attach the tamper-resistant housing 191 to the

composite member to cover the entire substrate. In the *McCalley et al.* reference, presumably it would be possible to remove the tamper-resistant housing 191 in an appropriate environment so that the sensor package 190 would expose signal lines and permit a probing of data by contacting the signal lines. This is because the circuit will operate normally even if the tamper-resistant housing 191, which is not necessary for the circuit operation, is removed. Thus, if a third party is familiar with the other light and power arrangements to destroy data, it may be possible to remove the housing and counteract such a destruction.

Our present invention as set forth in Claim 30 (amended) has the signal lines covered with only those components that are necessary for the circuit operation. If a component covering a signal line is removed, the circuit itself will be destroyed. Thus, during a normal operation, the multi-layer board of the present invention becomes extremely difficult to be subject to an unauthorized contact probing. The present invention not only provides its advantages in a distinct manner, it is also clearly defined by claim language that is neither anticipated or rendered obvious by the cited references.

In view of the above comments and the amendment to the claims, it is believed that the case is now in condition for allowance, and an early notification of the same is requested.

///

///

///

///

///

///

///

If the Examiner believes that a telephone interview will help further the prosecution of this case, she is respectfully requested to contact the undersigned attorney at the listed telephone number.

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on January 21, 2004.

By: James Lee

Signature

Dated: January 21, 2004

Very truly yours,

**SNELL & WILMER L.L.P.**

Joseph W. Price
Registration No. 25,124
1920 Main Street, Suite 1200
Irvine, California 92614-7230
Telephone: (949) 253-4920